

1c986 U.S. PTO
09/902309
07/10/01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Masahiro Kikuta et al. Art Unit : Unknown
Serial No. : Examiner : Unknown
Filed : July 10, 2001
Title : ELECTRONIC NOTARY METHOD AND SYSTEM

BOX PATENT APPLICATION

Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF PRIORITY DOCUMENT UNDER 35 USC §119

Applicant hereby confirms his claim of priority under 35 USC §119 from Japan
Application No. 2000-208913 filed July 10, 2000. A certified copy of the application from
which priority is claimed is submitted herewith.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 7-10-01

Y. Rocky Tsao
Y. Rocky Tsao
Reg. No. 34,053

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

20286323.doc

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL445371081US

I hereby certify under 37 CFR §1.10 that this correspondence is being
deposited with the United States Postal Service as Express Mail Post
Office to Addressee with sufficient postage on the date indicated below
and is addressed to the Commissioner for Patents, Washington,
D.C. 20231.

July 10, 2001
Date of Deposit
Samantha Bell
Signature

Samantha Bell
Typed or Printed Name of Person Signing Certificate

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC986 U.S. PTO
09/902309
07/10/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 7月10日

出 願 番 号

Application Number:

特願2000-208913

出 願 人

Applicant (s):

亜細亜証券印刷株式会社

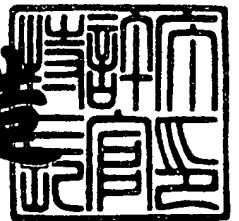
株式会社シナジー・インキュベート

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年10月20日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3087401

【書類名】 特許願

【整理番号】 A000002778

【提出日】 平成12年 7月10日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00

【発明の名称】 電子公証システムおよび電子公証方法

【請求項の数】 16

【発明者】

 【住所又は居所】 東京都渋谷区富ヶ谷一丁目30番22号 株式会社シナ
ジュー・インキュベート内

 【氏名】 菊田 昌弘

【発明者】

 【住所又は居所】 東京都渋谷区富ヶ谷一丁目30番22号 株式会社シナ
ジュー・インキュベート内

 【氏名】 渡邊 修

【特許出願人】

 【住所又は居所】 東京都港区虎ノ門1丁目25番7号

 【氏名又は名称】 亜細亜証券印刷株式会社

【特許出願人】

 【住所又は居所】 東京都渋谷区富ヶ谷一丁目30番22号

 【氏名又は名称】 株式会社 シナジュー・インキュベート

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子公証システムおよび電子公証方法

【特許請求の範囲】

【請求項 1】 公証サーバと、この公証サーバとネットワーク通信が可能な第 1 の端末装置および第 2 の端末装置とからなる電子公証システムにおいて、
前記第 1 の端末装置は、

ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、

前記ユーザを識別する第 1 のユーザ識別情報を入力する入力手段と、

前記公証サーバより予め与えられた第 2 のユーザ識別情報を用いて、前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記メッセージデータと、前記入力手段より入力された第 1 のユーザ識別情報を前記公証サーバに送信し、登録鍵を受信する第 1 の端末側通信手段とを備え、

前記公証サーバは、

前記ユーザの第 1 のユーザ識別情報と、前記ユーザに予め与えた第 2 のユーザ識別情報に対応づけて記憶する第 1 の記憶手段と、

前記第 1 の端末側通信手段より送られる第 2 のユーザ識別情報と、前記第 1 の記憶手段に記憶される第 2 のユーザ識別情報が一致する場合に、前記第 1 の端末側通信手段との間に通信リンクを開設し通信する第 1 の通信手段と、

この第 1 の通信手段を通じて前記第 1 の端末装置よりメッセージデータを受信すると、登録鍵を生成し、前記第 1 の通信手段を通じて前記第 1 の端末装置に送信する登録鍵生成手段と、

前記第 1 の通信手段を通じて受信した第 1 のユーザ識別情報と、前記第 1 の記憶手段に記憶される第 1 のユーザ識別情報が一致する場合に、前記第 1 の通信手段を通じて受信したメッセージデータを、少なくとも前記登録鍵と日時情報に対応づけて記憶する第 2 の記憶手段とを備え、

前記第 2 の端末装置は、

電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、

前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記メッセージデータと登録鍵を前記公証サーバに送信する第2の端末側通信手段を備え、

前記公証サーバは、

前記第2の端末側通信手段との間に通信リンクを開設し通信する第2の通信手段と、

この第2の通信手段を通じて受信した前記メッセージデータと、前記第2の記憶手段に記憶され、前記第2の通信手段を通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、前記第2の通信手段を通じて前記第2の端末装置に送信する公証情報生成手段とを具備することを特徴とする電子公証システム。

【請求項2】 前記第1の端末装置は、

ユーザが指定する電子ファイルと、この電子ファイルに基づいて生成されたメッセージデータと、前記電子ファイルに対応する登録鍵を一体化した謄本情報を生成し、前記第1の端末側通信手段を通じて前記公証サーバに送信する謄本生成手段を備え、

前記公証サーバは、

前記第1の通信手段を通じて受信した前記謄本情報に含まれる情報に対応づけて、請求鍵を生成する請求鍵生成手段と、

前記第1の通信手段を通じて受信した前記謄本情報に含まれるメッセージデータと、前記第2の記憶手段に記憶され、前記謄本情報に含まれる登録鍵に対応するメッセージデータとが一致し、なおかつ前記第1の通信手段を通じて受信した第1のユーザ識別情報と、前記第1の記憶手段に記憶される第1のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを前記請求鍵に対応づけて謄本ファイルとして記憶する第3の記憶手段を備え、

前記第2の端末装置は、

請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記第2の端末側通信手段を通じて前記公証サーバに送信する謄本要求手段を備え、

前記公証サーバは、

前記第 2 の通信手段を通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記第 3 の記憶手段より読み出して、前記第 2 の通信手段を通じて前記第 2 の端末装置に送信する謄本ファイル送信制御手段とを備えることを特徴とする請求項 1 に記載の電子公証システム。

【請求項 3】 公証サーバと、この公証サーバとネットワーク通信が可能な第 1 の端末装置および第 2 の端末装置とからなる電子公証システムにおいて、

前記第 1 の端末装置は、

前記ユーザを識別する第 1 のユーザ識別情報を入力する入力手段と、

ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成手段と、

前記公証サーバより予め与えられた第 2 のユーザ識別情報を用いて、前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記謄本情報と、前記入力手段より入力された第 1 のユーザ識別情報を前記公証サーバに送信する第 1 の端末側通信手段とを備え、

前記公証サーバは、

前記ユーザの第 1 のユーザ識別情報と、前記ユーザに予め与えた第 2 のユーザ識別情報を対応づけて記憶する第 1 の記憶手段と、

前記第 1 の端末側通信手段より送られる第 2 のユーザ識別情報と、前記第 1 の記憶手段に記憶される第 2 のユーザ識別情報が一致する場合に、前記第 1 の端末側通信手段との間に通信リンクを開設し通信する第 1 の通信手段と、

この第 1 の通信手段を通じて受信した前記謄本情報に含まれる電子ファイルに対応づけて、請求鍵を生成する請求鍵生成手段と、

前記第 1 の通信手段を通じて受信した第 1 のユーザ識別情報と、前記第 1 の記憶手段に記憶される第 1 のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを、少なくとも前記請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第 3 の記憶手段を備え、

前記第 2 の端末装置は、

前記公証サーバとの間に通信リンクを開設して通信する第 2 の端末側通信手段と、

請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記第 2 の端末側

通信手段を通じて前記公証サーバに送信する謄本要求手段を備え、

前記公証サーバは、

前記第 2 の端末側通信手段との間に通信リンクを開設し通信する第 2 の通信手段と、

この第 2 の通信手段を通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記第 3 の記憶手段より読み出して、前記第 2 の通信手段を通じて前記第 2 の端末装置に送信する謄本ファイル送信制御手段とを備えることを特徴とする電子公証システム。

【請求項 4】 前記ネットワーク上に、前記請求鍵を取得可能な Web を有する Web サーバを備え、

前記公証サーバは、

前記第 1 の端末装置より指定される電子メールアドレス宛てに、前記 Web の URL 情報を電子メールにて送信する URL 情報通知手段を備えることを特徴とする請求項 2 または請求項 3 に記載の電子公証システム。

【請求項 5】 前記謄本ファイル送信制御手段が電子ファイルを前記第 2 の端末装置に送信した場合に、前記第 2 の端末装置から謄本要求情報を受信した時刻と、前記電子ファイルを前記第 2 の端末装置に送信した時刻のうち、少なくとも一方を記憶する第 4 の記憶手段を備えることを特徴とする請求項 2 または請求項 3 に記載の電子公証システム。

【請求項 6】 前記第 1 のユーザ識別情報は、前記ユーザのバイオメトリック情報であることを特徴とする請求項 1 乃至請求項 5 のいずれかに記載の電子公証システム。

【請求項 7】 公証サーバと、この公証サーバとネットワーク通信が可能な端末装置とからなる電子公証システムにおいて、

前記端末装置は、

ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、

前記ユーザを識別する第 1 のユーザ識別情報を入力する入力手段と、

前記公証サーバより予め与えられた第 2 のユーザ識別情報を用いて、前記公

証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記メッセージデータと、前記入力手段より入力された第 1 のユーザ識別情報を前記公証サーバに送信し、登録鍵を受信する端末側通信手段とを備え、

前記公証サーバは、

前記ユーザの第 1 のユーザ識別情報と、前記ユーザに予め与えた第 2 のユーザ識別情報を対応づけて記憶する第 1 の記憶手段と、

前記端末側通信手段より送られる第 2 のユーザ識別情報と、前記第 1 の記憶手段に記憶される第 2 のユーザ識別情報が一致する場合に、前記端末側通信手段との間に通信リンクを開設し通信する通信手段と、

この通信手段を通じて前記端末装置よりメッセージデータを受信すると、登録鍵を生成し、前記通信手段を通じて前記端末装置に送信する登録鍵生成手段と

前記通信手段を通じて受信した第 1 のユーザ識別情報と、前記第 1 の記憶手段に記憶される第 1 のユーザ識別情報が一致する場合に、前記通信手段を通じて受信したメッセージデータを、少なくとも前記登録鍵と日時情報に対応づけて記憶する第 2 の記憶手段とを具備することを特徴とする電子公証システム。

【請求項 8】 公証サーバと、この公証サーバとネットワーク通信が可能な端末装置とからなる電子公証システムにおいて、

前記端末装置は、

電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、

前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記メッセージデータと登録鍵を前記公証サーバに送信する端末側通信手段を備え、

前記公証サーバは、

電子ファイルのメッセージデータを、少なくとも登録鍵と日時情報に対応づけて記憶する記憶手段と、

前記端末側通信手段との間に通信リンクを開設し通信する通信手段と、

この通信手段を通じて受信した前記メッセージデータと、前記記憶手段に記

憶され、前記通信手段を通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、前記通信手段を通じて前記端末装置に送信する公証情報生成手段とを具備することを特徴とする電子公証システム。

【請求項 9】 公証サーバと、この公証サーバとネットワーク通信が可能な端末装置とからなる電子公証システムにおいて、

前記端末装置は、

前記ユーザを識別する第 1 のユーザ識別情報を入力する入力手段と、

ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成手段と、

前記公証サーバより予め与えられた第 2 のユーザ識別情報を用いて、前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記謄本情報と、前記入力手段より入力された第 1 のユーザ識別情報を前記公証サーバに送信する端末側通信手段とを備え、

前記公証サーバは、

前記ユーザの第 1 のユーザ識別情報と、前記ユーザに予め与えた第 2 のユーザ識別情報に対応づけて記憶する第 1 の記憶手段と、

前記端末側通信手段より送られる第 2 のユーザ識別情報と、前記第 1 の記憶手段に記憶される第 2 のユーザ識別情報が一致する場合に、前記端末側通信手段との間に通信リンクを開設し通信する通信手段と、

この通信手段を通じて受信した前記謄本情報に含まれる電子ファイルに対応づけて、請求鍵を生成する請求鍵生成手段と、

前記通信手段を通じて受信した第 1 のユーザ識別情報と、前記第 1 の記憶手段に記憶される第 1 のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを、少なくとも前記請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第 2 の記憶手段とを具備することを特徴とする電子公証システム。

【請求項 10】 公証サーバと、この公証サーバとネットワーク通信が可能な端末装置とからなる電子公証システムにおいて、

前記端末装置は、

前記公証サーバとの間に通信リンクを開設して通信する端末側通信手段と、
請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記端末側通信手段を通じて前記公証サーバに送信する謄本要求手段を備え、

前記公証サーバは、

電子ファイルを、少なくとも請求鍵と日時情報に対応づけて謄本ファイルとして記憶する記憶手段を備え、

前記端末側通信手段との間に通信リンクを開設し通信する通信手段と、

この通信手段を通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記記憶手段より読み出して、前記通信手段を通じて前記端末装置に送信する謄本ファイル送信制御手段とを具備することを特徴とする電子公証システム。

【請求項 1 1】 公証サーバと、この公証サーバとネットワーク通信が可能な第 1 の端末装置および第 2 の端末装置とからなる電子公証システムで用いられる電子公証方法において、

前記公証サーバが、前記第 1 の端末装置のユーザの第 1 のユーザ識別情報と、前記ユーザに予め与えた第 2 のユーザ識別情報を対応づけて記憶する第 1 の記憶工程と、

前記第 1 の端末装置が、前記ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成工程と、

前記第 1 の端末装置が、前記ユーザを識別する第 1 のユーザ識別情報を受け付ける受付工程と、

前記第 1 の端末装置が、前記公証サーバより予め与えられた第 2 のユーザ識別情報を前記公証サーバに送信し、この第 2 のユーザ識別情報が前記公証サーバにおいて、前記第 1 の記憶工程にて記憶された第 2 のユーザ識別情報と一致する場合に、前記第 1 の端末装置と前記公証サーバの間に前記第 1 の通信リンクを開設する第 1 の通信リンク開設工程と、

前記第 1 の端末装置が前記公証サーバに対して、前記第 1 の通信リンクを通じて、少なくとも前記固有メッセージ生成工程にて生成したメッセージデータと、前記受付工程にて受け付けた第 1 のユーザ識別情報を送信する公証登録要求工程

と、

前記公証サーバが、前記第 1 の通信リンクを通じて前記第 1 の端末装置よりメッセージデータを受信すると、登録鍵を生成し、前記第 1 の通信リンクを通じて前記第 1 の端末装置に送信する登録鍵生成工程と、

前記公証サーバが、前記第 1 の通信リンクを通じて受信した前記第 1 のユーザ識別情報と、前記第 1 の記憶工程で記憶される第 1 のユーザ識別情報が一致する場合に、前記第 1 の通信リンクを通じて受信したメッセージデータを、少なくとも前記登録鍵と日時情報に対応づけて記憶する第 2 の記憶工程と、

前記第 2 の端末装置が、電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成工程と、

前記第 2 の端末装置と前記公証サーバとの間に第 2 の通信リンクを開設して通信する第 2 の通信リンク開設工程と、

前記第 2 の端末装置が、前記第 2 の通信リンクを通じて、少なくとも前記メッセージデータと登録鍵を前記公証サーバに送信する公証要求工程と、

前記公証サーバが、前記第 2 の通信リンクを通じて受信した前記メッセージデータと、前記第 2 の記憶工程にて記憶され前記第 2 の通信リンクを通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、前記第 2 の通信リンクを通じて前記第 2 の端末装置に送信する公証情報生成工程とを具備することを特徴とする電子公証方法。

【請求項 1 2】 前記第 1 の端末装置が、ユーザが指定する電子ファイルと、この電子ファイルに基づいて生成されたメッセージデータと、前記電子ファイルに対応する登録鍵を一体化した謄本情報を生成し、前記第 1 の通信リンクを通じて前記公証サーバに送信する謄本生成工程と、

前記公証サーバが、前記第 1 の通信リンクを通じて受信した前記謄本情報に含まれる情報に対応づけて、請求鍵を生成する請求鍵生成工程と、

前記公証サーバが、前記第 1 の通信リンクを通じて受信した前記謄本情報に含まれるメッセージデータと、前記第 2 の記憶工程にて記憶され前記謄本情報に含まれる登録鍵に対応するメッセージデータとが一致し、なおかつ前記第 1 の通信リンクを通じて受信した第 1 のユーザ識別情報と、前記第 1 の記憶工程にて記憶

される第1のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを前記請求鍵に対応づけて謄本ファイルとして記憶する第3の記憶工程と、

前記第2の端末装置が、請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記公証サーバに送信する謄本要求工程と、

前記公証サーバが、前記第2の端末装置より受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記第3の記憶工程で記憶した情報より読み出して、前記第2の端末装置に送信する謄本ファイル送信工程とを備えることを特徴とする請求項11に記載の電子公証方法。

【請求項13】 公証サーバと、この公証サーバとネットワーク通信が可能な第1の端末装置および第2の端末装置とからなる電子公証システムで用いられる電子公証方法において、

前記公証サーバが、前記第1の端末装置のユーザの第1のユーザ識別情報と、前記ユーザに予め与えた第2のユーザ識別情報に対応づけて記憶する第1の記憶工程と、

前記第1の端末装置が、前記ユーザを識別する第1のユーザ識別情報を受け付ける受付工程と、

前記第1の端末装置が、ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成工程と、

前記第1の端末装置が、前記公証サーバより予め与えられた第2のユーザ識別情報を前記公証サーバに送信し、この第2のユーザ識別情報が前記公証サーバにおいて、前記第1の記憶工程にて記憶された第2のユーザ識別情報と一致する場合に、前記第1の端末装置と前記公証サーバの間に前記第1の通信リンクを開設する第1の通信リンク開設工程と、

前記第1の端末装置が前記公証サーバに対して、前記第1の通信リンクを通じて、少なくとも前記謄本生成工程にて生成した謄本情報と、前記受付工程にて受け付けた第1のユーザ識別情報を送信する謄本登録要求工程と、

前記公証サーバが、前記第1の通信リンクを通じて前記第1の端末装置より謄本情報を受信すると、請求鍵を生成する請求鍵生成工程と、

前記公証サーバが、前記第 1 の通信リンクを通じて受信した第 1 のユーザ識別情報と、前記第 1 の記憶工程で記憶される第 1 のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを、少なくとも前記請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第 3 の記憶工程と、

前記第 2 の端末装置と前記公証サーバとの間に第 2 の通信リンクを開設して通信する第 2 の通信リンク開設工程と、

前記第 2 の端末装置が、前記第 2 の通信リンクを通じて、請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記公証サーバに送信する謄本要求工程と、

前記公証サーバが、前記第 2 の通信リンクを通じて受信した前記謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記第 3 の記憶工程にて記憶した情報より読み出して、前記第 2 の通信リンクを通じて前記第 2 の端末装置に送信する謄本ファイル送信工程とを備えることを特徴とする電子公証方法。

【請求項 1 4】 前記ネットワーク上に、前記請求鍵を取得可能な Web を有する Web サーバを備え、

前記公証サーバにおいて、前記第 1 の端末装置より指定される電子メールアドレス宛てに、前記 Web の URL 情報を電子メールにて送信する URL 情報通知工程を備えることを特徴とする請求項 1 2 または請求項 1 3 に記載の電子公証方法。

【請求項 1 5】 前記謄本ファイル送信工程が電子ファイルを前記第 2 の端末装置に送信した場合に、前記第 2 の端末装置から謄本要求情報を受信した時刻と、前記電子ファイルを前記第 2 の端末装置に送信した時刻のうち、少なくとも一方を記憶する第 4 の記憶工程を備えることを特徴とする請求項 1 2 または請求項 1 3 に記載の電子公証方法。

【請求項 1 6】 前記第 1 のユーザ識別情報は、前記ユーザのバイオメトリック情報であることを特徴とする請求項 1 1 乃至請求項 1 5 のいずれかに記載の電子公証方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、例えばインターネットなどのコンピュータネットワークを通じて、電子化された文書の公証を行う電子公証システムに関する。

【0002】

【従来の技術】

周知のように、近時、インターネットなどのコンピュータネットワークを通じて契約や商取引などが行われるようになり、今後、このようなネットワーク利用は、さらに発展すると見込まれている。このようなネットワーク利用を支える認証技術の1つとして、電子署名がある。

【0003】

この電子署名は、ネットワーク上でやりとりされるデジタル情報に署名情報を付加して、デジタル情報の正当性を保証する技術で、署名には公開鍵暗号が用いられる。この公開鍵は、認証局（CA：Certificate Authority）といわれる第三者機関により、その正当性が保証される。

【0004】

以下、図7を参照して、その一例を説明する。

【0005】

署名者（送信者）は、送信する文書Mからハッシュ関数hを用いて特徴値を生成し、これと自分だけが知っている秘密鍵から署名文D（h（M））を作る。そして、署名文D（h（M））と元の文書Mと一緒に相手に送る。

【0006】

これに対して、検証者（受信者）は、受け取った署名文D（h（M））を署名者の公開鍵で解き、上記h（M）を得る。また、受信した元の文書Mをハッシュ関数hで圧縮し、この圧縮結果h（M）と、上述のように公開鍵で解いたh（M）を比較して、署名が正しいかどうかを検査することにより、受信した文書Mの正当性を確認する。

【0007】

この他に、文書の送信者を識別する方法として、虹彩認証や声紋認証、サイン鑑定などの認証技術も開発されている。

以上のような認証技術を用いて、電子化された文書に電子署名して保証を行うことにより、悪意のある第三者が正当な署名者になりすまして、文書を偽造することが防止できる。

【0008】

しかしながら、例えば同一の取引に関して正当な署名者が、複数の異なる内容の文書に電子署名を行った場合、どの文書が正しい文書であるか確認する必要がある。

【0009】

さらに、このように複数の異なる内容の署名文書が存在する場合に、例えば遺言状のように署名者本人によって確認が行えないものの際には、どの文書が正当なものであるかを確認できないという問題が生じる。

【0010】

【発明が解決しようとする課題】

従来の技術では、ネットワーク上でやりとりされる文書を公証するには不十分であるという問題があった。

この発明は上記の問題を解決すべくなされたもので、ネットワーク上でやりとりされる文書に対して、信頼性の高い公証を行うことが可能な電子公証システムおよび電子公証方法を提供することを目的とする。

【0011】

【課題を解決するための手段】

上記の目的を達成するために、請求項1に係わる本発明は、公証サーバと、この公証サーバとネットワーク通信が可能な第1の端末装置および第2の端末装置とからなる電子公証システムにおいて、第1の端末装置は、ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、ユーザを識別する第1のユーザ識別情報を入力する入力手段と、公証サーバより予め与えられた第2のユーザ識別情報を用いて、公証サーバとの間に通信リンクを開設して通信するもので、少なくともメッセージデータと、入力手段より入力された第1のユーザ識別情報を公証サーバに送信し、登録鍵を受信する第1の端末側通信手段とを備え、公証サーバは、ユーザの第1のユー

ザ識別情報と、ユーザに予め与えた第2のユーザ識別情報を対応づけて記憶する第1の記憶手段と、第1の端末側通信手段より送られる第2のユーザ識別情報と、第1の記憶手段に記憶される第2のユーザ識別情報が一致する場合に、第1の端末側通信手段との間に通信リンクを開設し通信する第1の通信手段と、この第1の通信手段を通じて第1の端末装置よりメッセージデータを受信すると、登録鍵を生成し、第1の通信手段を通じて第1の端末装置に送信する登録鍵生成手段と、第1の通信手段を通じて受信した第1のユーザ識別情報と、第1の記憶手段に記憶される第1のユーザ識別情報が一致する場合に、第1の通信手段を通じて受信したメッセージデータを、少なくとも登録鍵と日時情報に対応づけて記憶する第2の記憶手段とを備え、第2の端末装置は、電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、公証サーバとの間に通信リンクを開設して通信するもので、少なくともメッセージデータと登録鍵を公証サーバに送信する第2の端末側通信手段を備え、公証サーバは、第2の端末側通信手段との間に通信リンクを開設し通信する第2の通信手段と、この第2の通信手段を通じて受信したメッセージデータと、第2の記憶手段に記憶され、第2の通信手段を通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、第2の通信手段を通じて第2の端末装置に送信する公証情報生成手段とを具備して構成するようにした。

【 0 0 1 2 】

また、請求項11に係わる本発明は、公証サーバと、この公証サーバとネットワーク通信が可能な第1の端末装置および第2の端末装置とからなる電子公証システムで用いられる電子公証方法において、公証サーバが、第1の端末装置のユーザの第1のユーザ識別情報と、ユーザに予め与えた第2のユーザ識別情報を対応づけて記憶する第1の記憶工程と、第1の端末装置が、ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成工程と、第1の端末装置が、ユーザを識別する第1のユーザ識別情報を受け付ける受付工程と、第1の端末装置が、公証サーバより予め与えられた第2のユーザ識別情報を公証サーバに送信し、この第2のユーザ識別情報が公証サーバ

バにおいて、第 1 の記憶工程にて記憶された第 2 のユーザ識別情報と一致する場合に、第 1 の端末装置と公証サーバの間に第 1 の通信リンクを開設する第 1 の通信リンク開設工程と、第 1 の端末装置が公証サーバに対して、第 1 の通信リンクを通じて、少なくとも固有メッセージ生成工程にて生成したメッセージデータと、受付工程にて受け付けた第 1 のユーザ識別情報を送信する公証登録要求工程と、公証サーバが、第 1 の通信リンクを通じて第 1 の端末装置よりメッセージデータを受信すると、登録鍵を生成し、第 1 の通信リンクを通じて第 1 の端末装置に送信する登録鍵生成工程と、公証サーバが、第 1 の通信リンクを通じて受信した第 1 のユーザ識別情報と、第 1 の記憶工程で記憶される第 1 のユーザ識別情報が一致する場合に、第 1 の通信リンクを通じて受信したメッセージデータを、少なくとも登録鍵と日時情報に対応づけて記憶する第 2 の記憶工程と、第 2 の端末装置が、電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成工程と、第 2 の端末装置と公証サーバとの間に第 2 の通信リンクを開設して通信する第 2 の通信リンク開設工程と、第 2 の端末装置が、第 2 の通信リンクを通じて、少なくとも前記メッセージデータと登録鍵を公証サーバに送信する公証要求工程と、公証サーバが、第 2 の通信リンクを通じて受信したメッセージデータと、第 2 の記憶工程にて記憶され第 2 の通信リンクを通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、第 2 の通信リンクを通じて第 2 の端末装置に送信する公証情報生成工程とを具備して構成するようにした。

【 0 0 1 3 】

上記構成の電子公証システムおよび電子公証方法では、電子ファイルの公証登録を行なう場合には、第 1 の端末装置にて、予め与えられたユーザ識別情報を用いて公証サーバとの間に通信リンクを開設し、公証対象となる電子ファイルの固有のメッセージデータを作成して公証サーバに送信する。

【 0 0 1 4 】

これに対して公証サーバは、第 1 の端末装置よりメッセージデータを受信すると、登録鍵を作成し、第 1 の端末装置から送られるバイオメトリック情報などの第 1 のユーザ識別情報に基づいて、第 1 の端末装置のユーザが正当な者であるこ

とを識別すると、上記登録鍵を上記電子ファイルに対応づけて記憶する。

【0015】

一方、手元の電子ファイルが公証されたものであるか確認する場合には、第2の端末装置により、上記電子ファイルの固有のメッセージデータを作成し、このメッセージデータと、電子ファイルとともに入手した登録鍵を公証サーバに送信する。

【0016】

これに対して、公証サーバは、受信した登録鍵に対応するメッセージデータを読み出し、このメッセージデータと、第2の端末装置より受信したメッセージデータが一致する場合には、その旨を示す公証情報を作成し、第2の端末装置に送信するようにしている。

【0017】

したがって、上記構成の電子公証システムおよび電子公証方法によれば、悪意を有する第三者が、第1の端末装置のユーザになりすまして電子ファイルを公証登録しようとしても、上記ユーザの識別情報や、バイオメトリック情報などの第1のユーザ識別情報の入力が必要なため、なりすましによる不正公証登録を確実に防止できる。

【0018】

すなわち、上記構成の電子公証システムおよび電子公証方法によれば、公証サーバにより公証される電子ファイルは、公証人役場で公証される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、公証確認を求める者はネットワークを通じて迅速かつ正確な公証サービスを受けることができる。

【0019】

そしてまた、請求項3に係わる本発明は、公証サーバと、この公証サーバとネットワーク通信が可能な第1の端末装置および第2の端末装置とからなる電子公証システムにおいて、第1の端末装置は、ユーザを識別する第1のユーザ識別情報を入力する入力手段と、ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成手段と、公証サーバより予め与えられた第2のユーザ識別情報を用いて、公証サーバとの間に通信リンクを開設して通信するもので、少なくとも謄

本情報と、入力手段より入力された第 1 のユーザ識別情報を公証サーバに送信する第 1 の端末側通信手段とを備え、公証サーバは、ユーザの第 1 のユーザ識別情報と、ユーザに予め与えた第 2 のユーザ識別情報を対応づけて記憶する第 1 の記憶手段と、第 1 の端末側通信手段より送られる第 2 のユーザ識別情報と、第 1 の記憶手段に記憶される第 2 のユーザ識別情報が一致する場合に、第 1 の端末側通信手段との間に通信リンクを開設し通信する第 1 の通信手段と、この第 1 の通信手段を通じて受信した謄本情報に含まれる電子ファイルに対応づけて、請求鍵を生成する請求鍵生成手段と、第 1 の通信手段を通じて受信した第 1 のユーザ識別情報と、第 1 の記憶手段に記憶される第 1 のユーザ識別情報が一致する場合に、謄本情報に含まれる電子ファイルを、少なくとも請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第 3 の記憶手段を備え、第 2 の端末装置は、公証サーバとの間に通信リンクを開設して通信する第 2 の端末側通信手段と、請求鍵を含む謄本要求情報を生成し、この謄本要求情報を第 2 の端末側通信手段を通じて公証サーバに送信する謄本要求手段を備え、公証サーバは、第 2 の端末側通信手段との間に通信リンクを開設し通信する第 2 の通信手段と、この第 2 の通信手段を通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、第 3 の記憶手段より読み出して、第 2 の通信手段を通じて第 2 の端末装置に送信する謄本ファイル送信制御手段を具備して構成するようにした。

【 0 0 2 0 】

さらにまた、請求項 1 3 に係わる本発明は、公証サーバと、この公証サーバとネットワーク通信が可能な第 1 の端末装置および第 2 の端末装置とからなる電子公証システムで用いられる電子公証方法において、公証サーバが、第 1 の端末装置のユーザの第 1 のユーザ識別情報と、ユーザに予め与えた第 2 のユーザ識別情報を対応づけて記憶する第 1 の記憶工程と、第 1 の端末装置が、ユーザを識別する第 1 のユーザ識別情報を受け付ける受付工程と、第 1 の端末装置が、ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成工程と、第 1 の端末装置が、公証サーバより予め与えられた第 2 のユーザ識別情報を公証サーバに送信し、この第 2 のユーザ識別情報が前記公証サーバにおいて、第 1 の記憶工程にて記憶された第 2 のユーザ識別情報と一致する場合に、第 1 の端末装置と公証サーバ

バの間に第1の通信リンクを開設する第1の通信リンク開設工程と、第1の端末装置が公証サーバに対して、第1の通信リンクを通じて、少なくとも謄本生成工程にて生成した謄本情報と、受付工程にて受け付けた第1のユーザ識別情報を送信する謄本登録要求工程と、公証サーバが、第1の通信リンクを通じて第1の端末装置より謄本情報を受信すると、請求鍵を生成する請求鍵生成工程と、公証サーバが、第1の通信リンクを通じて受信した第1のユーザ識別情報と、第1の記憶工程で記憶される第1のユーザ識別情報が一致する場合に、謄本情報に含まれる電子ファイルを、少なくとも請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第3の記憶工程と、第2の端末装置と前記サーバとの間に第2の通信リンクを開設して通信する第2の通信リンク開設工程と、第2の端末装置が、第2の通信リンクを通じて、請求鍵を含む謄本要求情報を生成し、この謄本要求情報を公証サーバに送信する謄本要求工程と、公証サーバが、第2の通信リンクを通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、第3の記憶工程にて記憶した情報より読み出して、第2の通信リンクを通じて第2の端末装置に送信する謄本ファイル送信工程とを具備して構成するようにした。

【0021】

上記構成の電子公証システムおよび電子公証方法では、電子ファイルの謄本登録を行なう場合には、第1の端末装置にて、予め与えられたユーザ識別情報を用いて公証サーバとの間に通信リンクを開設し、謄本となる電子ファイルを公証サーバに送信する。

【0022】

これに対して公証サーバは、第1の端末装置より電子ファイルを受信すると、請求鍵を作成し、第1の端末装置から送られるバイOMETリック情報などの第1のユーザ識別情報に基づいて、第1の端末装置のユーザが正当な者であることを識別すると、上記請求鍵を上記電子ファイルに対応づけて記憶する。

【0023】

一方、謄本登録された電子ファイルを取得する場合には、第2の端末装置より請求鍵を公証サーバに送信する。

これに対して、公証サーバは、受信した請求鍵に対応する電子ファイルを読み

出し、第2の端末装置に送信するようにしている。

【0024】

したがって、上記構成の電子公証システムおよび電子公証方法によれば、悪意を有する第三者が、第1の端末装置のユーザになりすまして電子ファイルを謄本登録しようとしても、上記ユーザの識別情報や、バイオメトリック情報などの第1のユーザ識別情報の入力が必要なため、なりすましによる不正謄本登録を確実に防止できる。

【0025】

すなわち、上記構成の電子公証システムおよび電子公証方法によれば、公証サーバに謄本登録された電子ファイルは、公証人役場で謄本登録される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、謄本の写しを求める者はネットワークを通じて迅速かつ正確な公証サービスを受けることができる。

【0026】

【発明の実施の形態】

以下、図面を参照して、この発明の一実施形態について説明する。

図1は、この発明の一実施形態に係わる電子公証システムの構成を示すものである。

【0027】

電子公証システムは、会員利用者端末100と、公証サーバ200と、一般利用者端末300とをからなり、これらは、インターネットなどのコンピュータネットワークを通じて接続される。

【0028】

会員利用者端末100は、公証サービスに加入した会員利用者が使用するパーソナルコンピュータであって、ネットワーク通信を実現するためのハードウェアと、ネットワーク上のメールサーバと電子メールを送受信するための電子メールソフトウェアや、ネットワーク上のWebサーバに蓄積されるデータを閲覧するブラウザソフトウェアを備える。この他、会員利用者端末100には、上記公証サービスを受けるための専用のクライアントソフトウェアがハードディスクなど

の記録媒体に組み込んである。

【 0 0 2 9 】

また、会員利用者端末 1 0 0 は、ネットワーク上で自己を証明するためのデジタル証明書を予め取得している。このデジタル証明書は、基本フォーマットが例えば I T U - T (Telecommunication Standardization Sector) の X. 5 0 9 に準拠するもので、認証サービスを提供する第三者機関にて発行されたものである。

【 0 0 3 0 】

さらに、会員利用者端末 1 0 0 は、パッド 1 0 1 を備える。パッド 1 0 1 は、サイン入力を行うための入力デバイスで、平板上に専用ペンで描かれたサインを電子データに変換する。そして、会員利用者端末 1 0 0 が、上記電子データに基づいて、上記サインの筆圧や速度をサイン情報として求める。

【 0 0 3 1 】

公証サーバ 2 0 0 は、当該公証サービスの中枢をなすサーバマシンであり、メールサーバ、Webサーバとしての機能を備える他、各会員のアカウント情報に対応づけて、デジタル証明書、サイン情報、電子メールアドレス、公証登録したファイルやそれに関連する種々の情報を記録可能なデータベース 2 0 1 を備える。

また、公証サーバ 2 0 0 は、ネットワークやGPS衛星、あるいは電波時計などより、高精度な時刻情報を取得する機能を持つ。

【 0 0 3 2 】

一般利用者端末 3 0 0 は、当該公証サービスにて公証された電子ファイルを取得した、あるいは取得した一般利用者が使用するパーソナルコンピュータであり、ネットワーク通信を実現するためのハードウェアと、ネットワーク上のメールサーバと電子メールを送受信するための電子メールソフトウェアや、ネットワーク上のWebサーバに蓄積されるデータを閲覧するブラウザソフトウェアを備える。

【 0 0 3 3 】

この他、一般利用者端末 3 0 0 は、公証要求や謄本請求を行うためのクライア

ントソフトウェアを、予め上記公証サービスより取得し、ハードディスクなどの記録媒体に組み込んでいる。

なお、一般利用者端末 3 0 0 は、上記クライアントソフトウェアが組み込まれた会員利用者端末 1 0 0 でも代用可能である。

【 0 0 3 4 】

次に、上記構成の電子公証システムの動作について説明する。

まず、当該公証サービスに会員登録済み（アカウント取得済み）の会員利用者が会員利用者端末 1 0 0 を通じて、任意の電子ファイルの公証情報を公証サーバ 2 0 0 に登録する際の動作について説明する。図 2 は、この際の会員利用者端末 1 0 0 および公証サーバ 2 0 0 の処理を模式的に示すものである。

【 0 0 3 5 】

会員利用者が、会員利用者端末 1 0 0 にてクライアントソフトウェアを起動すると、会員利用者端末 1 0 0 は、会員利用者に対して、当該公証サービスの加入時に予めアカウント登録したユーザ名（以下、ユーザ ID と称する）およびパスワードの入力を促す。

【 0 0 3 6 】

これに対して、会員利用者がユーザ ID およびパスワードをキーボード入力すると、会員利用者端末 1 0 0 は、ログイン処理を実行し、公証サーバ 2 0 0 との間に HTTP（Hyper Text Transport Protocol）による通信リンクを確立し、公証サーバ 2 0 0 に上記ユーザ ID およびパスワードを送信する。

【 0 0 3 7 】

上記ユーザ ID およびパスワードを受信した公証サーバ 2 0 0 は、受け取ったユーザ ID およびパスワードの組み合わせが正しいものであるか、データベース 2 0 1 内に記録される会員登録情報を参照して検証する。

【 0 0 3 8 】

そして、公証サーバ 2 0 0 は、受け取ったユーザ ID およびパスワードの組み合わせが正しいものであり、正当な会員利用者であることが確認されると、申請鍵を作成する。

【 0 0 3 9 】

この申請鍵は、当該申請鍵を特定するための申請鍵 I D と、上記会員利用者端末 1 0 0 がログインを行った日時（申請時刻）と、上記会員利用者のユーザ I D とからなり、会員利用者端末 1 0 0 に送信される。

【 0 0 4 0 】

これに対して、会員利用者端末 1 0 0 は、上記申請鍵を受信すると、公証申請の対象となる電子ファイルについての公証情報を作成する。

この公証情報には、上記電子ファイルに基づきメッセージダイジェスト技術により生成される固定長のメッセージをはじめ、上記電子ファイルについての情報（ファイル名、ファイルサイズ、最終変更日、コメント）、有効期限を示す情報が含まれる。

【 0 0 4 1 】

なお、以下の説明では、上記メッセージダイジェスト技術として、例えば RFC 1321 で規定される MD 5（Message Digest Algorithm 5）を用いる場合を例に説明する。

【 0 0 4 2 】

MD 5 は、一方向ハッシュ関数を使った演算により、元のデータの長さに関係なく 1 2 8 ビットのデータ（ハッシュ値）を作成するもので、このハッシュ値が上記固定長のメッセージとなる。

【 0 0 4 3 】

このようにして生成された、公証申請の対象となる電子ファイルについての公証情報は、公証サーバ 2 0 0 より受信した申請鍵 I D と組み合わせられて、1 つのパッケージとなり、登録情報として公証サーバ 2 0 0 に送信される。

【 0 0 4 4 】

公証サーバ 2 0 0 は、上記登録情報を受信すると、これより申請鍵 I D を取り出し、その正当性を検証する。

この検証の結果、取り出した申請鍵 I D が正当なものであることが分かると、上記登録情報内の情報に基づいて、登録鍵を作成する。

【 0 0 4 5 】

この登録鍵は、当該登録鍵を特定するための登録鍵 I D、上記会員利用者端末

100より登録情報を受信した日時（登録時刻）、上記申請鍵ID、上記登録情報内に含まれる電子ファイルの固定長のメッセージ（ハッシュ値）、電子ファイルについての情報（ファイル名、ファイルサイズ、最終変更日、コメント）、および有効期限を示す情報からなる。

そして、公証サーバ200は、登録鍵内の情報のうち、登録鍵IDを会員利用者端末100に送信する。

【0046】

これに対して、会員利用者端末100は、上記登録鍵IDを受信すると、会員利用者に対して、上記電子ファイルを公証登録してよいか、最終的な確認を行う。この確認は、パッド101を通じた署名入力により行われる。

会員利用者端末100は、パッド101より署名入力が行われると、これに基づくサイン情報を作成し、本人特定情報として公証サーバ200に送信する。

【0047】

公証サーバ200は、上記本人特定情報を受信すると、この本人特定情報が示す署名入力のサイン情報が本人の自署によるものであるかを判定する。この判定処理では、所定のアルゴリズムに従って、データベース201に予め記録される上記会員利用者の署名データと、上記サイン情報を比較することにより、その正当性の判定が行われる。

【0048】

ここで、本人の自署によるものであることが判ると、公証サーバ200は、上記申請鍵および登録鍵を公証情報としてデータベース201に登録し、会員利用者端末100との間の通信リンクを切断し、当該処理を終了する。

一方、会員利用者端末100では、公証サーバ200より受け取った登録鍵IDを保存する。

【0049】

次に、電子ファイルと登録鍵IDを入手した一般利用者が一般利用者端末300を通じて、上記電子ファイルが公証されたものであるか公証サーバ200に判定を求め、公証サーバ200が上記判定を行う際の動作について説明する。図3は、この際の一般利用者端末300および公証サーバ200の処理を模式的に示

すものである。

【 0 0 5 0 】

なお、公証サーバ 2 0 0 は、上記判定を求める端末からの接続要求については、一般利用者向けのクライアントソフトウェアが組み込まれている端末であれば、特に制限なく接続を許可する。

【 0 0 5 1 】

以下の説明では、一般利用者端末 3 0 0 と公証サーバ 2 0 0 との間に通信リンクを確立する処理については説明を省略し、通信リンクが確立された後の処理について説明する。

【 0 0 5 2 】

また、上記ソフトウェアが組み込まれていない端末が接続要求を行った場合には、上記端末に対して公証サーバ 2 0 0 は、上記一般利用者向けのクライアントソフトウェアのダウンロードを促し、要求に応じて上記ソフトウェアを提供する。

【 0 0 5 3 】

一般利用者端末 3 0 0 では、一般利用者が、当該公証サービスによって公証されたものであるか判定を求める電子ファイルと、それに対応する登録鍵 ID、および公証サーバ 2 0 0 との連絡に用いる電子メールアドレスを指定する。

【 0 0 5 4 】

すると、一般利用者端末 3 0 0 は、一般利用者に指定された電子ファイルに基づいて、MD 5 によるハッシュ値を求め、このハッシュ値と、上記指定された登録鍵 ID、電子メールアドレスを組み合わせ、公証要求情報として公証サーバ 2 0 0 に送信する。

【 0 0 5 5 】

上記公証要求情報を受信した公証サーバ 2 0 0 は、上記公証要求情報からハッシュ値と登録鍵 ID を取り出す。そして、この取り出した登録鍵 ID が、公証情報としてデータベース 2 0 1 に登録されているか否かを判定する。

【 0 0 5 6 】

ここで、登録が確認されると、公証サーバ 2 0 0 は、上記データベース 2 0 1

から上記登録鍵 I D に対応する公証情報内のハッシュ値を読み出し、上記公証要求情報から取り出したハッシュ値と一致するか検証する。

【 0 0 5 7 】

このようにして、登録鍵 I D の存在確認と、それに対応するハッシュ値の一致が確認されると、公証サーバ 2 0 0 は、これらの確認がなされた旨を示す確認情報を作成し、一般利用者端末 3 0 0 に送信するとともに、公証要求を受けた日時をデータベース 2 0 1 に記録する。

これに対して、一般利用者端末 3 0 0 は、確認情報を受信すると、公証サーバ 2 0 0 に対して当該電子ファイルの証明書の発行を要求（公証要求）する。

【 0 0 5 8 】

公証サーバ 2 0 0 は、上記公証要求を受け付けると、データベース 2 0 1 に記録される公証情報に基づいて、当該電子ファイルの証明書を作成する。なお、この証明書には、公証対象となった電子ファイルの公証登録の日時、登録者の氏名（ユーザ I D に対応する氏名）、ファイル名、ハッシュ値の他、書誌事項が含まれている。

そして、公証サーバ 2 0 0 は、作成した証明書を一般利用者端末 3 0 0 に送信し、これを一般利用者端末 3 0 0 が受信し、当該処理を終了する。

【 0 0 5 9 】

次に、会員利用者が会員利用者端末 1 0 0 を通じて、任意の電子ファイルの謄本を公証サーバ 2 0 0 に登録する際の動作について説明する。図 4 は、この際の会員利用者端末 1 0 0 および公証サーバ 2 0 0 の処理を模式的に示すものである。

【 0 0 6 0 】

なお、以下の説明では、会員利用者端末 1 0 0 と公証サーバ 2 0 0 との間に通信リンクを確立する処理については、図 2 の説明と同様であることより、説明を省略し、通信リンクが確立された後の処理について説明する。

【 0 0 6 1 】

会員利用者端末 1 0 0 では、会員利用者が、謄本として登録したい電子ファイルと、これに対応する登録鍵 I D（図 2 に示した処理で取得済）を指定すると、

会員利用者端末 1 0 0 は、上記電子ファイルから MD 5 によるハッシュ値を求め、このハッシュ値と、上記電子ファイルおよび登録鍵 ID をパッケージ化して、公証サーバ 2 0 0 に送信する。

【 0 0 6 2 】

パッケージを受信した公証サーバ 2 0 0 は、保存内容を確認する処理として、上記パッケージから登録鍵 ID とハッシュ値を取り出し、この登録鍵 ID が、①すでに公証サーバ 2 0 0 に登録されている登録鍵 ID と一致するか、②上記謄本登録要求した会員利用者によって登録されたものであるか、そして③取り出したハッシュ値が上記登録鍵 ID に対応する登録鍵内のハッシュ値と一致するか、④パッケージから取り出した電子ファイルから MD 5 によるハッシュ値を求め、このハッシュ値と一致するか、をそれぞれ検証する。

【 0 0 6 3 】

この検証の結果、上記条件①～④全てを満足することが確認されると、公証サーバ 2 0 0 は、保存準備処理として、上記パッケージ内の電子ファイルを仮保存するとともに、上記電子ファイルが登録鍵 ID に対応するものであることが確認できた旨を示す確認情報を作成し、これを会員利用者端末 1 0 0 に送信する。

【 0 0 6 4 】

これに対して、会員利用者端末 1 0 0 は、会員利用者に対して、上記電子ファイルを謄本として登録してよいか、最終的な確認を行う。この確認は、パッド 1 0 1 を通じた署名入力により行われる。

会員利用者端末 1 0 0 は、パッド 1 0 1 より署名入力が行われると、これに基づいてサイン情報を作成し、本人特定情報として公証サーバ 2 0 0 に送信する。

【 0 0 6 5 】

公証サーバ 2 0 0 は、上記本人特定情報を受信すると、この本人特定情報が示すサイン情報が本人の自署によるものであるかを判定する。この判定処理では、所定のアルゴリズムに従って、上記サイン情報を、データベース 2 0 1 に予め記録される署名データと比較することにより、その正当性の判定が行われる。

【 0 0 6 6 】

ここで、本人の自署によるものであることが判ると、公証サーバ 2 0 0 は、仮

保存していた電子ファイルを正式に謄本としてデータベース 2 0 1 に登録し、会員利用者端末 1 0 0 に登録の完了を通知して通信リンクを切断し、当該処理を終了する。

【 0 0 6 7 】

次に、会員利用者が会員利用者端末 1 0 0 を通じて公証サーバ 2 0 0 に対し、謄本として登録される電子ファイルを受け取るためのデータを一般利用者端末 3 0 0 に電子メールで送信させる際の動作について説明する。図 5 は、この際の会員利用者端末 1 0 0 および公証サーバ 2 0 0 の処理を模式的に示すものである。

【 0 0 6 8 】

なお、以下の説明では、会員利用者端末 1 0 0 と公証サーバ 2 0 0 との間に通信リンクを確立する処理については、図 2 の説明と同様であることより説明を省略し、通信リンクが確立された後の処理について説明する。

【 0 0 6 9 】

会員利用者端末 1 0 0 は、公証サーバ 2 0 0 との間に通信リンクが確立されると、保存しておいた所望の登録鍵 ID に、謄本取得を許可する一般利用者の電子メールアドレスと、有効期限、その他の制御情報を付加した送信情報を生成し、この送信情報を公証サーバ 2 0 0 に送信する。

【 0 0 7 0 】

上記送信情報を取得した公証サーバ 2 0 0 は、上記送信情報より登録鍵 ID を取り出し、この登録鍵 ID が、①すでに公証サーバ 2 0 0 に登録されている登録鍵 ID と一致するか、②上記謄本登録要求した会員利用者によって登録されたものであるか、をそれぞれ検証する。

【 0 0 7 1 】

この検証の結果、上記条件①、②共に満足することが確認されると、公証サーバ 2 0 0 は、請求鍵を作成する。

なお、この請求鍵は、当該請求鍵を特定するための請求鍵 ID と、会員利用者端末 1 0 0 より上記送信情報を受信した日時（登録時刻）、上記送信情報に含まれる登録鍵 ID、電子メールアドレス（送付先）、有効期限、その他の制御情報からなる。

【 0 0 7 2 】

また、上記送信情報にて複数の電子メールアドレスが指定される場合には、公証サーバ 2 0 0 は、その数だけ請求鍵を生成する。

そして、公証サーバ 2 0 0 は、会員利用者端末 1 0 0 に対して、上記請求鍵内の情報のうち、請求鍵 I D を確認情報として送信する。

【 0 0 7 3 】

これに対して、会員利用者端末 1 0 0 は、上記確認情報を受信すると、会員利用者に対して、上記電子ファイルの謄本取得を、電子メールアドレスで指定した一般利用者に許可してよいか、最終的な確認を行う。

【 0 0 7 4 】

この確認は、パッド 1 0 1 を通じた署名入力により行われる。

会員利用者端末 1 0 0 は、パッド 1 0 1 より署名入力が行われると、これに基づいてサイン情報を作成し、本人特定情報として公証サーバ 2 0 0 に送信する。

【 0 0 7 5 】

公証サーバ 2 0 0 は、上記本人特定情報を受信すると、この本人特定情報が示すサイン情報が本人の自署によるものであるかを判定する。この判定処理では、所定のアルゴリズムに従って、上記サイン情報を、データベース 2 0 1 に記録される署名データと比較することにより、その正当性の判定が行われる。

【 0 0 7 6 】

ここで、本人の自署によるものであることが判ると、公証サーバ 2 0 0 は、上記請求鍵を送信情報としてデータベース 2 0 1 に登録するとともに、上記請求鍵 I D を自己の持つ W e b 上に登録した後、会員利用者端末 1 0 0 に登録の完了を通知して通信リンクを切断する。なお、上記 W e b の U R L は、会員利用者端末 1 0 0 より通知された（送付先として指定された）上記電子メールアドレス毎に固有に設定されるものである。

【 0 0 7 7 】

そしてさらに、公証サーバ 2 0 0 は、上記電子メールアドレス宛てに、この電子メールアドレスに対応する上記 U R L の情報が含まれている電子メールを送信し、当該処理を終了する。

【 0 0 7 8 】

次に、一般利用者が一般利用者端末 3 0 0 を通じて、公証サーバ 2 0 0 に謄本登録される電子ファイルを取得する際の動作について説明する。図 6 は、この際の一般利用者端末 3 0 0 および公証サーバ 2 0 0 の処理を模式的に示すものである。

【 0 0 7 9 】

なお、公証サーバ 2 0 0 に謄本登録される電子ファイルを取得するには、図 2 の処理で発行された登録鍵 I D、あるいは図 5 の処理で生成された請求鍵 I D が必要となる。

【 0 0 8 0 】

その取得方法としては、一般利用者が、電子ファイルを謄本登録した利用者から直接取得することも考えられる。しかし、以下の説明では、当該システムでは最も一般的と考えられる、公証サーバ 2 0 0 の W e b より請求鍵 I D を取得する場合について説明する。

【 0 0 8 1 】

まず、一般利用者端末 3 0 0 は、図 5 に示した処理により公証サーバ 2 0 0 が送信する電子メールを受信すると、ブラウザソフトウェアを用いて、この電子メールに記載される U R L に対応する W e b の閲覧を開始する。そして、一般利用者端末 3 0 0 は、上記 W e b より請求鍵 I D を取得する。

【 0 0 8 2 】

上記 W e b は、図 5 でも示したように、公証サーバ 2 0 0 上に設けられており、一般利用者端末 3 0 0 により請求鍵 I D が取得されると、公証サーバ 2 0 0 は、その日時をデータベース 2 0 1 に記録する。

【 0 0 8 3 】

一方、一般利用者端末 3 0 0 では、一般利用者の要求に応じて、上記請求鍵 I D と自己の電子メールアドレスをパッケージ化して、謄本要求情報として公証サーバ 2 0 0 に送信する。

【 0 0 8 4 】

上記謄本要求情報を受信した一般利用者端末 3 0 0 は、上記謄本要求情報より

請求鍵IDと電子メールアドレスを取り出す。そして、この取り出した請求鍵IDと電子メールアドレスとが対応づけられて、送信情報としてデータベース201に登録されているか否かを判定する。

【0085】

ここで、登録が確認されると、公証サーバ200は、請求鍵IDの利用者が正当なものであると判断し、データベース201から上記請求鍵IDに対応する電子ファイルを読み出し、この電子ファイルからMD5によるハッシュ値を生成する。

【0086】

そして、公証サーバ200は、上記電子ファイル、上記ハッシュ値、上記電子ファイルの謄本登録日時、登録者、ファイル名、当該要求日時などの情報をパッケージ化し、謄本情報として一般利用者端末300に送信する。

【0087】

これに対して、一般利用者端末300は、受信した謄本情報から、電子ファイルを取り出し、この電子ファイルからMD5によるハッシュ値を生成する。そして、この生成したハッシュ値と、上記謄本情報内のハッシュ値を比較することにより、正常な受信がなされたかを確認する。

【0088】

ここで、正常な受信が確認されると、一般利用者端末300は、これらの確認がなされた旨を示す確認情報を作成して、公証サーバ200に送信し、公証サーバ200との間の通信リンクを切断し、当該処理を終了する。

【0089】

以上のように、上記構成の電子公証システムでは、公証サーバ200にて予め認証されているネットワークユーザ（会員利用者）が、公証対象となる電子ファイルの固有情報（ハッシュ値）を作成し、公証サーバ200は、サイン入力により上記ユーザが識別されると、上記固有情報と上記ユーザの識別情報を対応づけ、登録鍵IDとともに自己のデータベース201に保存し、上記登録鍵IDを上記ユーザにのみ報知する。

【0090】

そして、一般利用者（もしくは会員利用者）が、手元の電子ファイルが公証されたものであるか確認する場合には、上記電子ファイルよりハッシュ値を作成し、このハッシュ値と、電子ファイルとともに入手した登録鍵IDをネットワークを通じて公証サーバ200に送信し、公証されたものであるか確認要求を行う。

【0091】

これに対して、公証サーバ200は、受信した登録鍵IDに対応するハッシュ値をデータベース201より読み出し、このハッシュ値と、公証確認要求者より受信したハッシュ値が一致する場合には、その旨を示す公証情報を作成し、公証確認要求者に送信するようにしている。

【0092】

したがって、上記構成の電子公証システムによれば、悪意を有する第三者が、会員利用者になりすまして電子ファイルを公証登録しようとしても、会員利用者のユーザIDやパスワード、サイン入力によるユーザ識別情報を入力する必要があるため、なりすましによる不正公証登録を確実に防止できる。

【0093】

すなわち、公証サーバ200により公証される電子ファイルは、公証人役場で公証される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、公証確認要求者はネットワークを通じて迅速かつ正確な公証サービスを受けることができる。

【0094】

また、公証サーバ200は、電子ファイルのハッシュ値を公証情報としてデータベース201に記録するにあたり、会員利用者から公証登録の要求があった日時の情報をあわせて記録するようにしているので、同じ会員利用者から同一の取引などに関して複数の登録がなされた場合でも、その要求日時より有効な電子ファイルを識別することができる。

【0095】

さらに、上記構成の電子公証システムでは、公証サーバ200に対して、すでに公証されている電子ファイルと、そのハッシュ値を送信して、会員利用者が謄本登録を要求すると、サイン入力による本人識別後、公証サーバ200は、受信

した電子ファイルを謄本として登録する。

【 0 0 9 6 】

上記会員利用者が、公証サーバ 2 0 0 に対して謄本の送付要求を行うと、公証サーバ 2 0 0 は、上記謄本を取得可能な請求鍵 ID を載せた Web を作成し、上記送付要求にて指定される電子メールアドレス宛てに、上記 Web の URL を通知する電子メールを送信する。

【 0 0 9 7 】

そして、上記電子メールを取得したネットワークユーザ（一般利用者もしくは会員利用者）は、ブラウザソフトウェアを用いて、上記 Web を閲覧して、請求鍵 ID を取得し、これを用いて謄本を取得し、これに対して公証サーバ 2 0 0 は、この取得がなされた日時を記録するようにしている。

【 0 0 9 8 】

したがって、上記構成の電子公証システムによれば、悪意を有する第三者が、会員利用者になりすまして電子ファイルを謄本登録しようとしても、会員利用者のユーザ ID やパスワード、サイン入力によるユーザ識別情報を入力する必要があるため、なりすましによる不正な謄本登録を確実に防止できる。

【 0 0 9 9 】

すなわち、公証サーバ 2 0 0 に謄本登録される電子ファイルは、公証人役場で公証される紙媒体の公正証書と同様に、真正性が保証された謄本が登録されたものであり、謄本の提供要求者はネットワークを通じて迅速かつ正確に謄本を取得することができる。

【 0 1 0 0 】

また、公証サーバ 2 0 0 は、電子ファイルの公証、および電子ファイルの謄本を提供するにあたり、ネットワークユーザから公証要求や謄本提供の要求があった日時をデータベース 2 0 1 に記録するようにしているので、これらの要求の発生を把握することができる。また、上述のように要求のあった日時だけでなく、公証の証明を発行した日時や、謄本を提供した日時を記録するようにしてもよい。

【 0 1 0 1 】

尚、この発明は上記実施の形態に限定されるものではない。例えば、上記実施の形態では、図4に示したように、電子ファイルの謄本としての登録処理は、図2に示した処理により、予め公証登録を行った後に行うものとして説明したが、これに限定されるものではない。

【0102】

例えば、図2に示した処理において、会員利用者端末100が登録情報内に謄本登録したい電子ファイルを含めて送信し、そして、所定の条件を満たす場合に、公証サーバ200が登録鍵IDを発行するようにしてもよい。

【0103】

このように、電子ファイルの謄本登録に先立って予め公証登録しない構成であっても、悪意を有する第三者が、会員利用者になりすまして電子ファイルを謄本登録することは不可能であり、なりすましによる不正な謄本登録を確実に防止できる。

【0104】

また、図6に示した謄本の提供処理では、電子メールにて通知されるURLに対応するWebを参照して請求鍵IDを入手し、これを用いて謄本を取得するものとして説明したが、これに限定されるものではない。

【0105】

例えば、何らなの方法により登録鍵IDを取得したネットワークユーザからの要求に応じて、謄本を提供するようにしてもよい。なお、この場合には、要求者に対して、第三者により認証されたデジタル証明書や、電子メールアドレスの通知を要求し、これらの情報と、予めデータベース201に記憶しておいた許可される者の情報を参照し、一致が確認された場合にのみ謄本を提供することにより、不正な謄本取得を防止できる。また、これらの設定を、謄本の登録者が任意に設定するようにしてもよい。

【0106】

さらに、上記実施の形態では、会員利用者の認証を、パッド101を通じたサイン入力で行うものと説明したが、これに代わって例えば、虹彩認証や声紋認証、指紋認証などのバイオメトリック認証や、その他、ICカードによる個人認証

を適用することも可能である。

【0107】

さらにまた、会員利用者端末100および一般利用者端末300は、通常のパーソナルコンピュータを利用可能である。そして、この実施形態で説明した各端末の処理は、それぞれ組み込まれるクライアントソフトウェアを、上記パーソナルコンピュータが搭載するマイクロプロセッサが実行し、ネットワーク通信機能を利用して実現できる。

【0108】

このため、ネットワーク通信可能なパーソナルコンピュータを所有する者であれば、上記クライアントソフトウェアを組み込むだけ、上記公証サービスの恩恵を受けることができる。

【0109】

そしてまた、上記実施の形態では、会員利用者端末および一般利用者端末の各クライアント端末は、ハードディスクに組み込んだクライアントソフトウェアに基づいて動作するものとした。

これに代わり例えば、クライアント端末から要求が生じるたびに、公証サーバが上記要求に該当するJ A V A アプレットを提供し、クライアント端末は、提供された上記アプレットに基づいて、上記クライアントソフトウェアと同様の処理動作を実現するようにしてもよい。このような構成によれば、予めクライアント端末がクライアントソフトウェアを入手したり、公証サーバよりダウンロードする必要がない。

【0110】

また、申請鍵ID、登録鍵IDおよび請求鍵IDは、例えばR S A (Rivest-S hamir-Adleman Scheme) 方式により暗号化処理を施して生成するものとしてもよい。

その他、この発明の要旨を逸脱しない範囲で種々の変形を施しても同様に実施可能であることはいうまでもない。

【0111】

【発明の効果】

以上述べたように、この発明では、電子ファイルの公証登録を行なう場合には、第 1 の端末装置にて、予め与えられた第 2 のユーザ識別情報を用いて公証サーバとの間に通信リンクを開設し、公証対象となる電子ファイルの固有のメッセージデータを作成して公証サーバに送信する。

【 0 1 1 2 】

これに対して公証サーバは、第 1 の端末装置よりメッセージデータを受信すると、登録鍵を作成し、第 1 の端末装置から送られる第 1 のユーザ識別情報に基づいて、第 1 の端末装置のユーザが正当な者であることを識別すると、上記登録鍵を上記電子ファイルに対応づけて記憶する。

【 0 1 1 3 】

一方、手元の電子ファイルが公証されたものであるか確認する場合には、第 2 の端末装置により、上記電子ファイルの固有のメッセージデータを作成し、このメッセージデータと、電子ファイルとともに入手した登録鍵を公証サーバに送信する。

【 0 1 1 4 】

これに対して、公証サーバは、受信した登録鍵に対応するメッセージデータを読み出し、このメッセージデータと、第 2 の端末装置より受信したメッセージデータが一致する場合には、その旨を示す公証情報を作成し、第 2 の端末装置に送信するようにしている。

【 0 1 1 5 】

したがって、この発明によれば、悪意を有する第三者が、第 1 の端末装置のユーザになりすまして電子ファイルを公証登録しようとしても、上記ユーザの識別情報や、バイオメトリック情報などの第 1 のユーザ識別情報の入力が必要なため、なりすましによる不正公証登録を確実に防止できる。

【 0 1 1 6 】

すなわち、公証サーバにより公証される電子ファイルは、公証人役場で公証される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、公証確認を求める者はネットワークを通じて迅速かつ正確な公証サービスを受けることが可能な電子公証システムおよび電子公証方法を提供できる。

【0117】

また、この発明では、電子ファイルの謄本登録を行なう場合には、第1の端末装置にて、予め与えられた第2のユーザ識別情報を用いて公証サーバとの間に通信リンクを開設し、謄本となる電子ファイルを公証サーバに送信する。

【0118】

これに対して公証サーバは、第1の端末装置より電子ファイルを受信すると、請求鍵を作成し、第1の端末装置から送られる第1のユーザ識別情報に基づいて、第1の端末装置のユーザが正当な者であることを識別すると、上記請求鍵を上記電子ファイルに対応づけて記憶する。

【0119】

一方、謄本登録された電子ファイルを取得する場合には、第2の端末装置より請求鍵を公証サーバに送信する。

これに対して、公証サーバは、受信した請求鍵に対応する電子ファイルを読み出し、第2の端末装置に送信するようにしている。

【0120】

したがって、この発明によれば、悪意を有する第三者が、第1の端末装置のユーザになりすまして電子ファイルを謄本登録しようとしても、第2のユーザ識別情報や、バイオメトリック情報をはじめとする第1のユーザ識別情報情報の入力が必要なため、なりすましによる不正謄本登録を確実に防止できる。

【0121】

すなわち、公証サーバに謄本登録された電子ファイルは、公証人役場で謄本登録される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、謄本の写しを求める者はネットワークを通じて迅速かつ正確な公証サービスを受けることが可能な電子公証システムおよび電子公証方法を提供できる。

【図面の簡単な説明】

【図1】

この発明に係わる電子公証システムの一実施形態の構成を示す図。

【図2】

図1に示した電子公証システムにおける、電子ファイルの公証情報の登録処理

を説明するための図。

【図 3】

図 1 に示した電子公証システムにおける、電子ファイルの公証確認処理を説明するための図。

【図 4】

図 1 に示した電子公証システムにおける、電子ファイルの謄本登録処理を説明するための図。

【図 5】

図 1 に示した電子公証システムにおける、電子ファイルの謄本送信要求処理を説明するための図。

【図 6】

図 1 に示した電子公証システムにおける、電子ファイルの謄本提供処理を説明するための図。

【図 7】

電子署名技術を説明するための図。

【符号の説明】

1 0 0 … 会員利用者端末

1 0 1 … パッド

2 0 0 … 公証サーバ

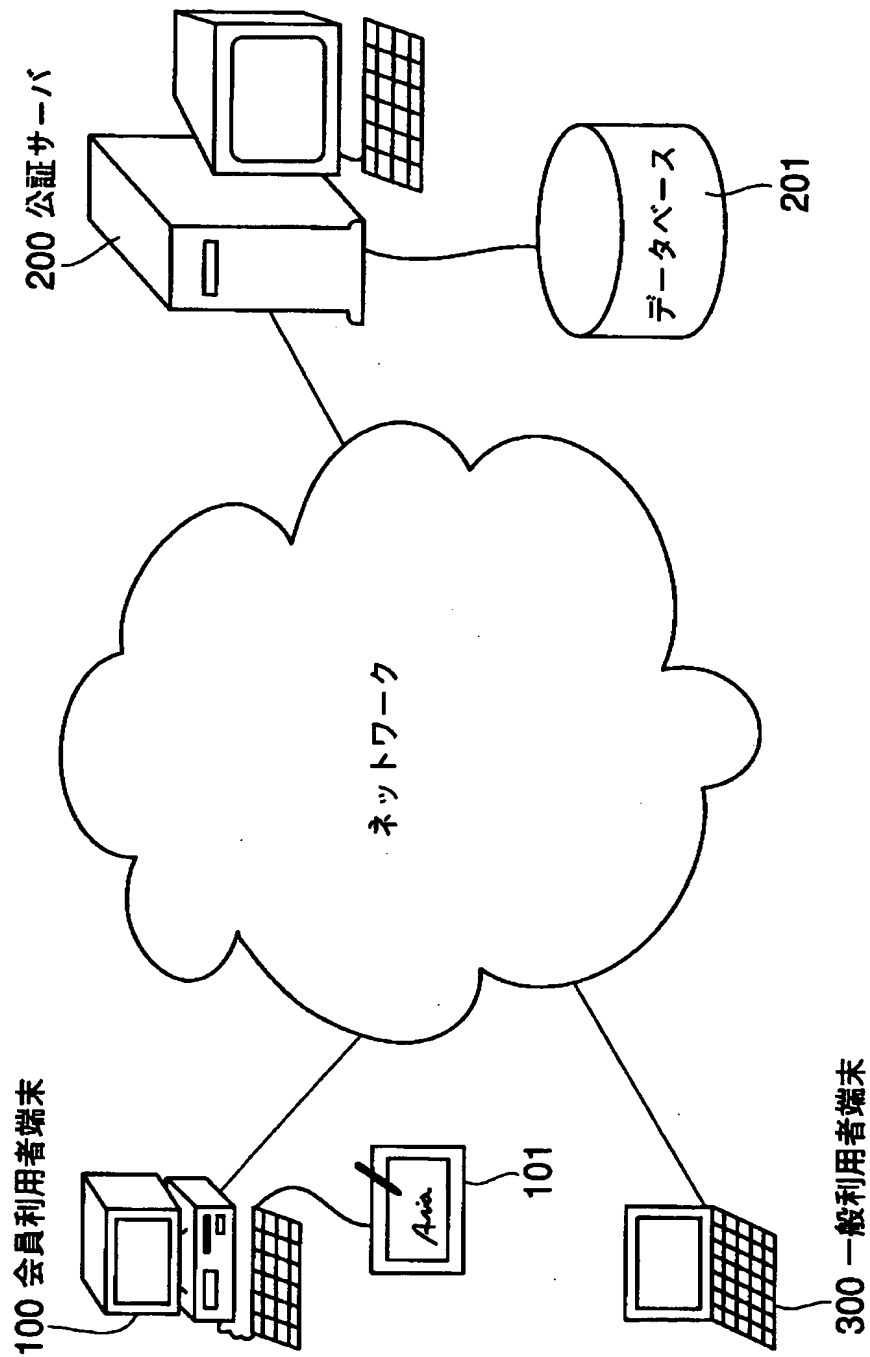
2 0 1 … データベース

3 0 0 … 一般利用者端末

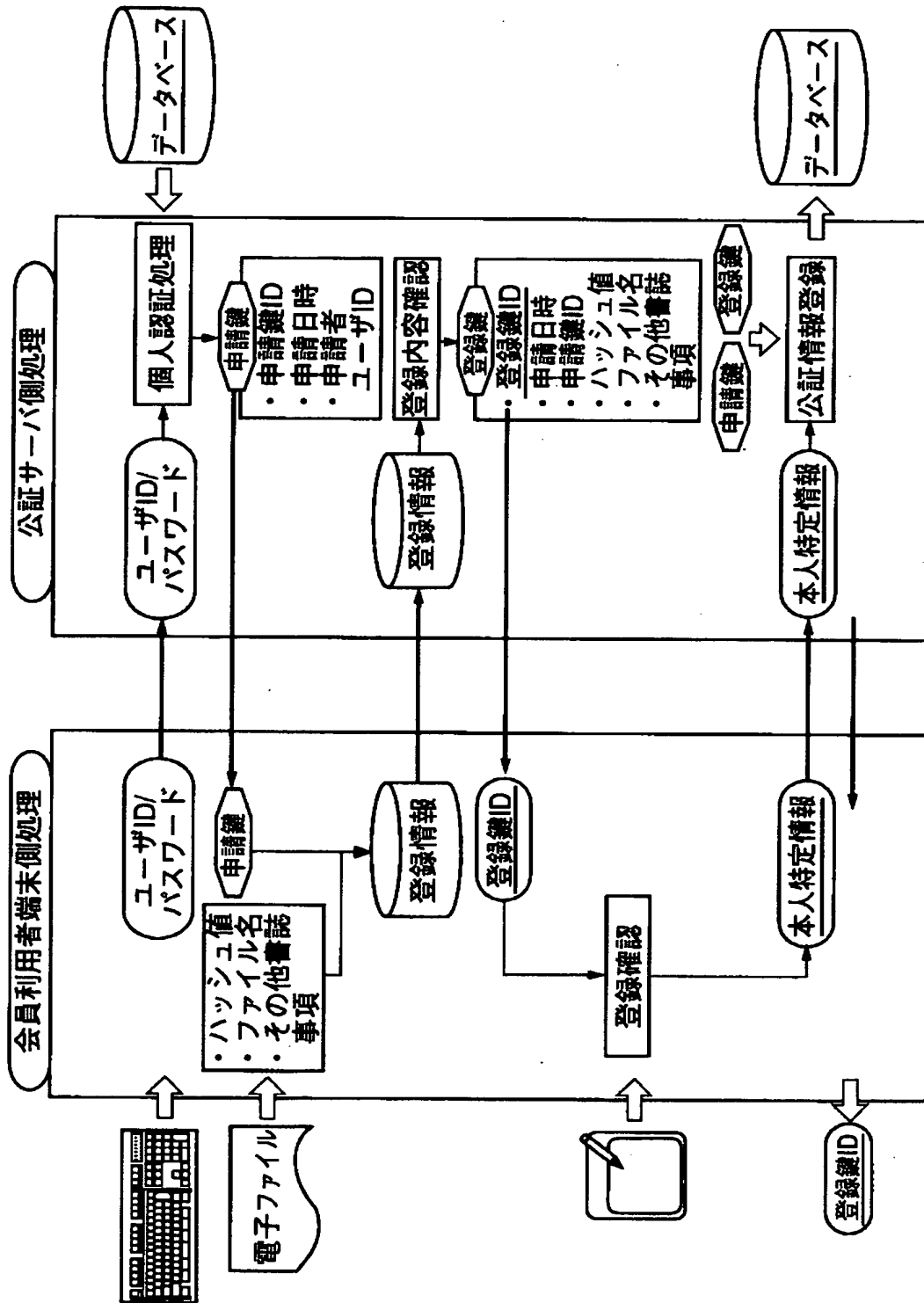
【書類名】

図面

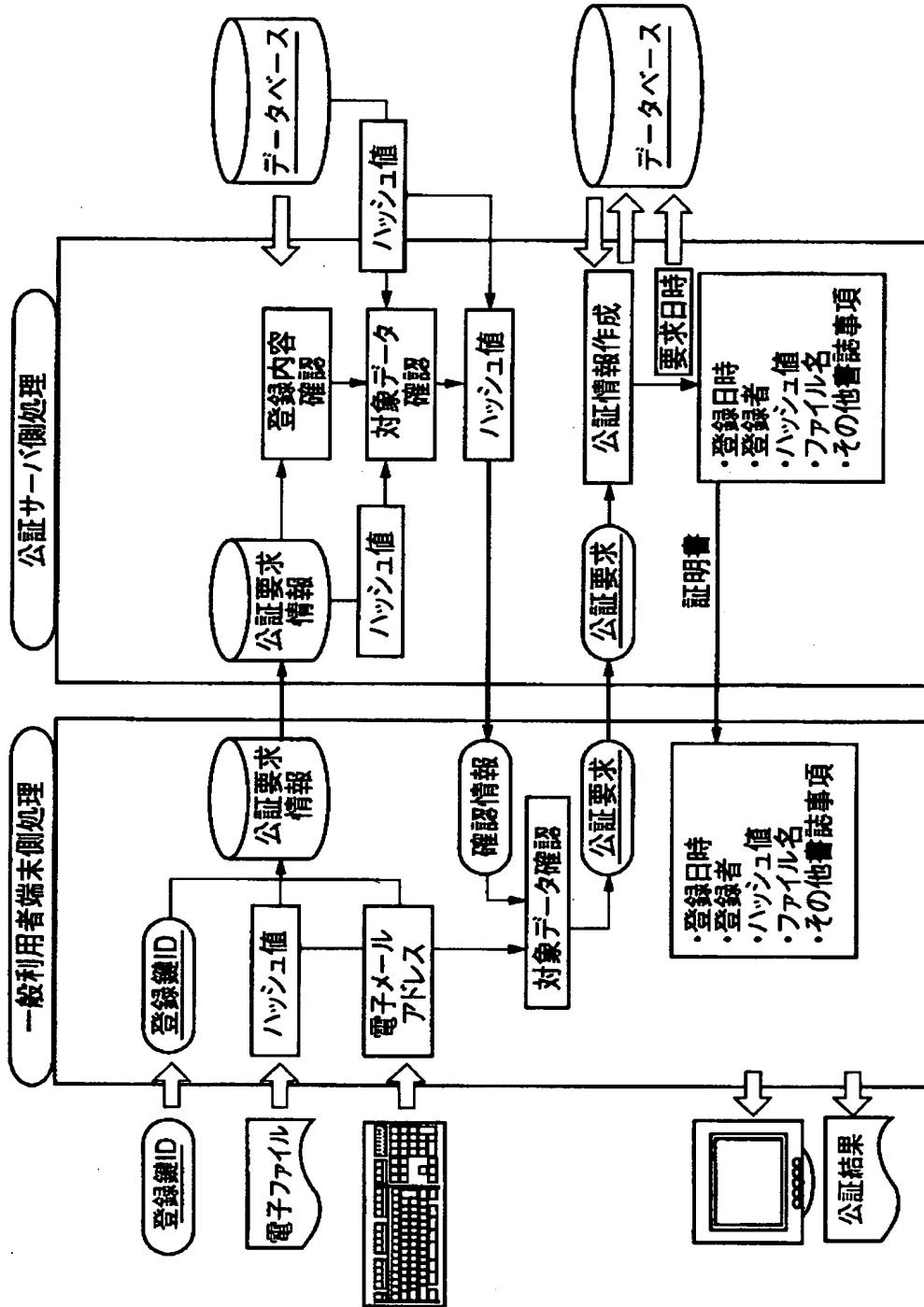
【図 1】



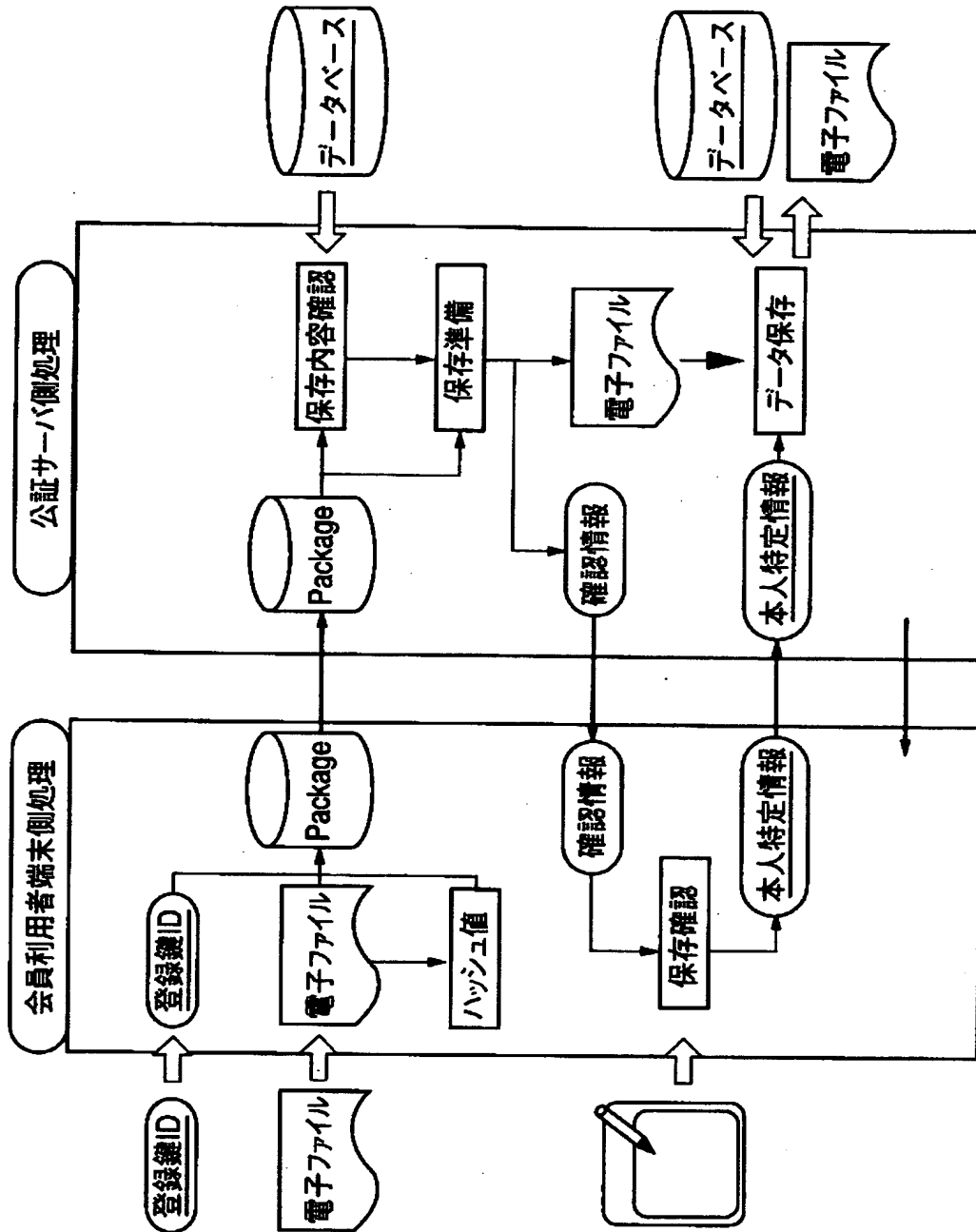
【図2】



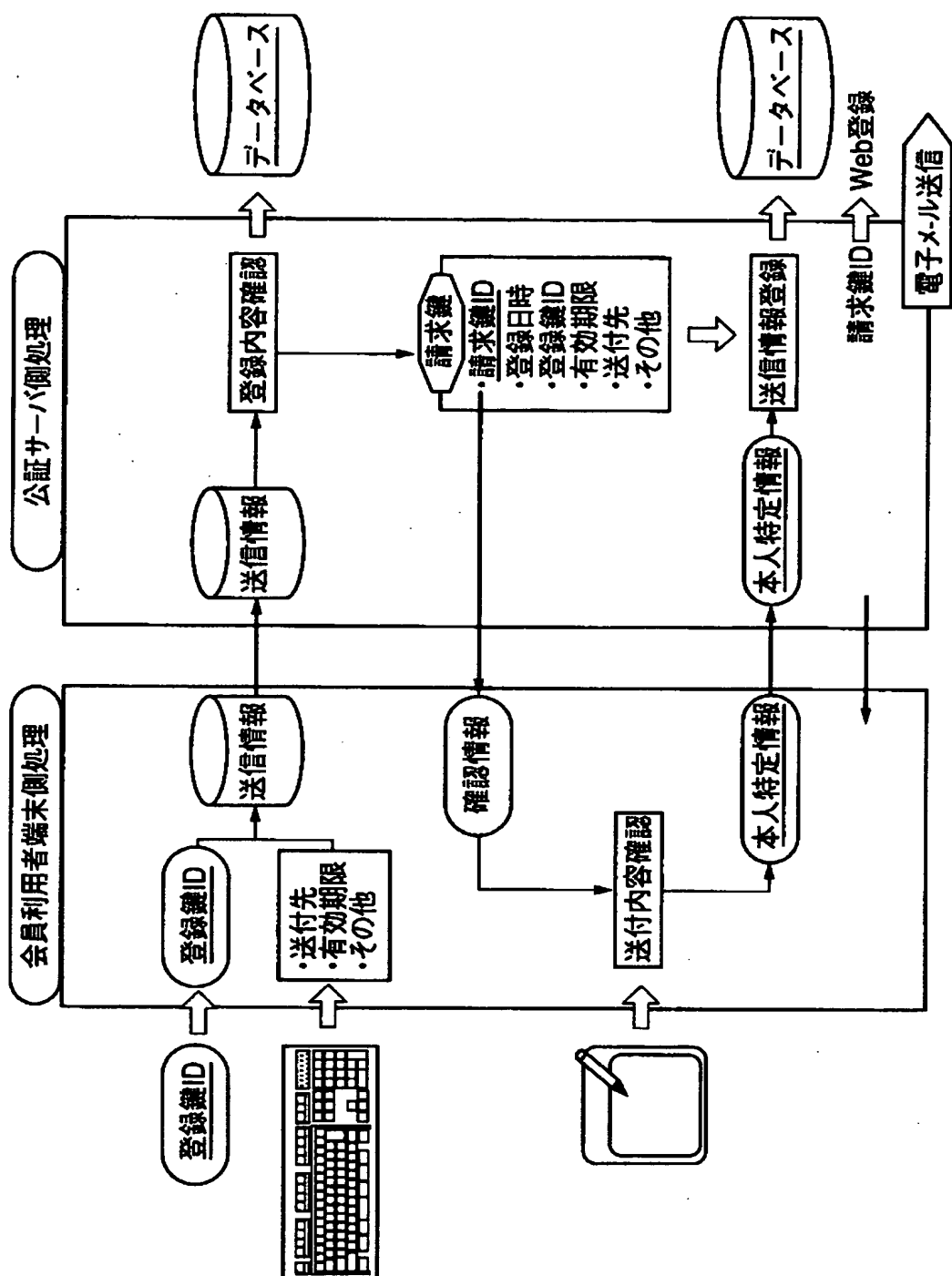
【図 3】



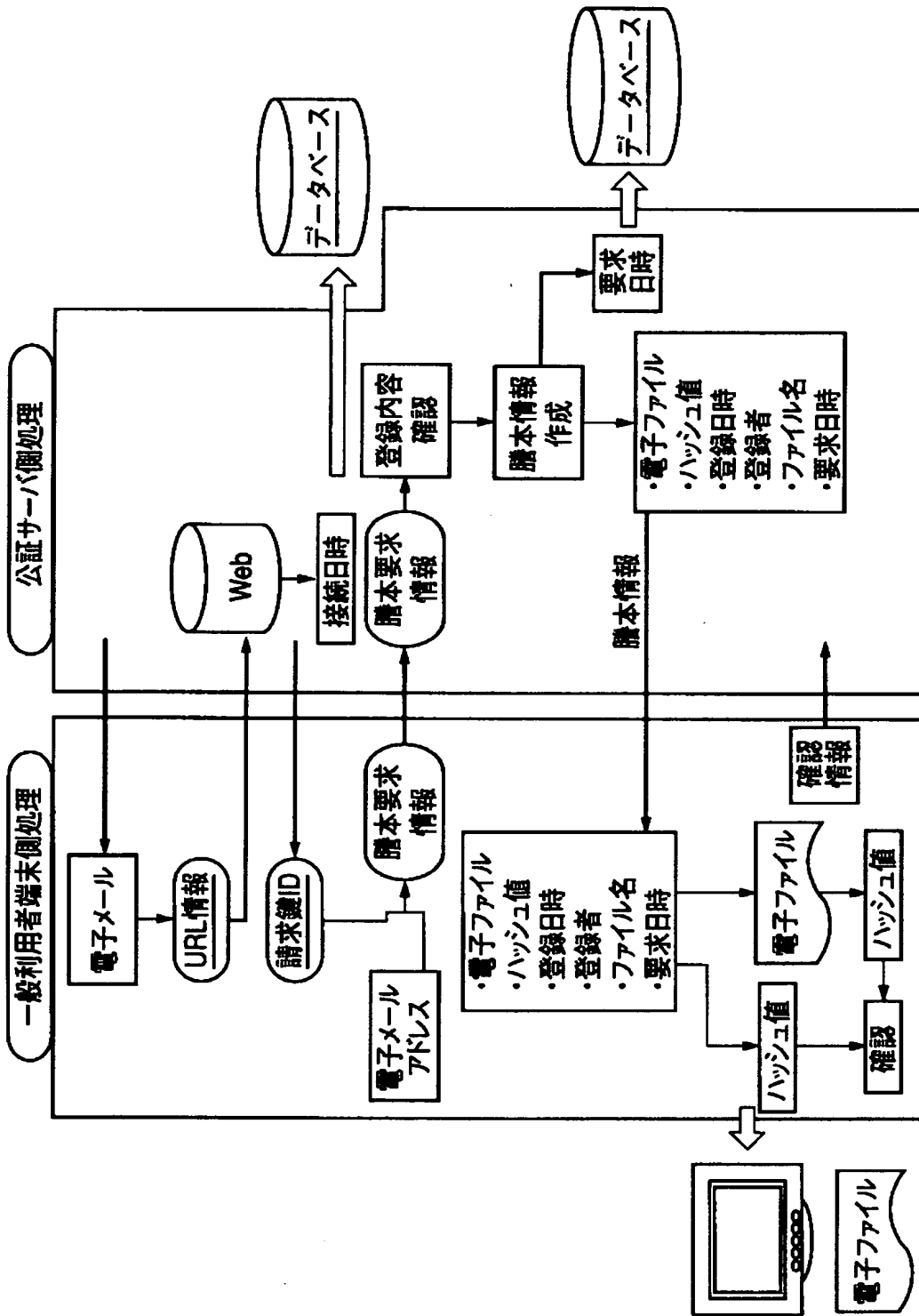
【図 4】



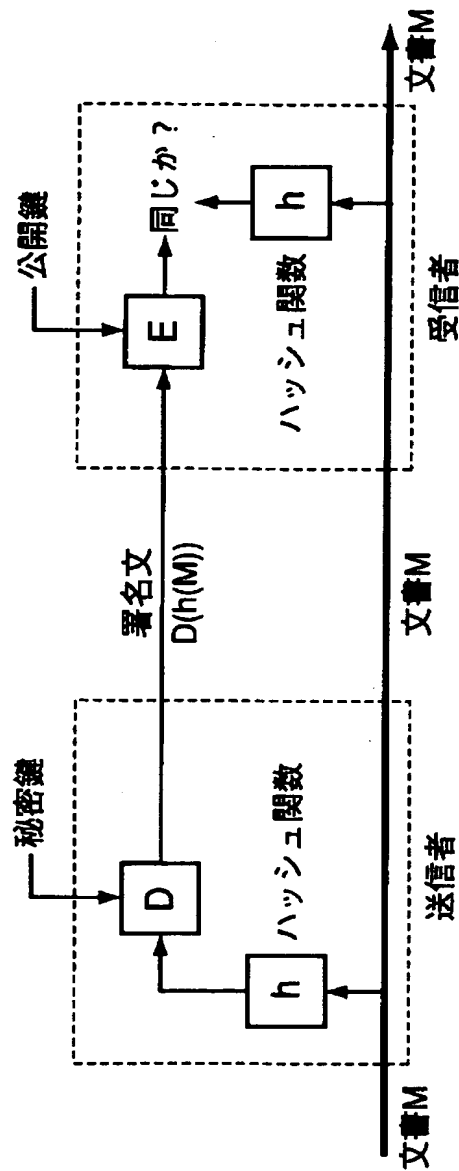
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 ネットワーク上でやりとりされる文書に対して、信頼性の高い公証を行うことが可能な電子公証システムおよび電子公証方法を提供する。

【解決手段】 会員利用者は会員利用者端末 1 0 0 にて、公証対象となる電子ファイルの固有情報を作成し、公証サーバ 2 0 0 は、サイン入力により上記会員利用者を識別すると、上記固有情報と会員利用者の識別情報を対応づけ、登録鍵 ID とともにデータベース 2 0 1 に保存し、登録鍵 ID を会員利用者に送信する。一般利用者が、上記電子ファイルの公証確認を行う場合には、一般利用者端末 3 0 0 を用いて、上記電子ファイルより固有情報を作成し、上記電子ファイルとともに入手した登録鍵 ID とともに公証サーバ 2 0 0 に送信する。これに対して、公証サーバ 2 0 0 は、受信した固有情報と、データベース 2 0 1 の固有情報が一致する場合に、公証情報を一般利用者に送信するようにしたものである。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 0 - 2 0 8 9 1 3
受付番号	5 0 0 0 0 8 6 8 0 7 4
書類名	特許願
担当官	高田 良彦 2 3 1 9
作成日	平成 1 2 年 7 月 1 7 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	597095599
【住所又は居所】	東京都港区虎ノ門 1 - 2 5 - 7
【氏名又は名称】	亜細亜証券印刷株式会社

【特許出願人】

【識別番号】	500324783
【住所又は居所】	東京都渋谷区富ヶ谷一丁目 3 0 番 2 2 号
【氏名又は名称】	株式会社シナジー・インキュベート

【代理人】

【識別番号】	100058479
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外 國特許法律事務所内
【氏名又は名称】	鈴江 武彦

【選任した代理人】

【識別番号】	100084618
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外 國特許法律事務所内
【氏名又は名称】	村松 貞男

【選任した代理人】

【識別番号】	100068814
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外 國特許法律事務所内
【氏名又は名称】	坪井 淳

【選任した代理人】

【識別番号】	100092196
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外 國特許法律事務所内
【氏名又は名称】	橋本 良郎

次頁有

認定・付加情報（続き）

【選任した代理人】

【識別番号】 100091351

【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外
國特許法律事務所内

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外
國特許法律事務所内

【氏名又は名称】 中村 誠

出 願 人 履 歴 情 報

識別番号 [597095599]

1. 変更年月日 1997年 6月23日
[変更理由] 新規登録
住 所 東京都港区虎ノ門1-25-7
氏 名 亜細亜証券印刷株式会社

出 願 人 履 歴 情 報

識別番号 [500324783]

1. 変更年月日 2000年 7月10日
[変更理由] 新規登録
住 所 東京都渋谷区富ヶ谷一丁目30番22号
氏 名 株式会社シナジー・インキュベート